PTO/SB/21

U.S. Department of Commerce
Patent and Trademark Office
PATENT

APPEAL BRIEF TRANSMITTAL

Mail Stop Appeal-Brief Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Customer No.: 23696
Attorney Docket No.: 010055B1
In Re Application of: Roy Quick et al.
Serial Number: 09/863,139
Filed: May 22, 2001
Examiner: Moorthy, Aravind K.
Group Art Unit: 2131

Dear Sir:

Transmitted herewith for filing is a Notice of Appeal in the above identified application.

EXTENSION FEES	☐ One Month	$120	$
	☐ Two Months	$450	$
	☐ Three Months	$1020	$
	☒ Four Months	$ 1,590.00	$1,590.00
APPEAL BRIEF		$500	$500.00
TERMINAL DISCLAIMER		$130	$
		TOTAL FEE	$2,090.00

4. ☐ Fee check in the amount of $_____ is enclosed to pay for any claim and/or extension fees.
5. ☒ Please charge Deposit Account No. 17-0026 of QUALCOMM Incorporated the amount of $2,090.00
   The Commissioner is hereby authorized to charge payment of any additional fees that may be required, or credit any overpayment to said Deposit Account No. 17-0026. A duplicate of this sheet is enclosed for fee processing.
6. ☒ The Commissioner is further hereby authorized to charge to said Deposit Account No. 17-0026, pursuant to 37 CFR 1.25(b), any fee whatsoever which may become properly due or payable, as set forth in 37 CFR 1.16 to 37 CFR 1.18 inclusive, for the entire pendency of this application without specific additional authorization.

Date: August 24, 2006

Signature: David Hoffman Reg. No. 56771 for
Jac-Hee Choi, Reg. No. 45,288
(858) 651-5469

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-5787
Facsimile: (858) 658-2502

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8(a))

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

☐ deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Depositor's Name: _____
(type or print name)

Date: _____

FACSIMILE

☒ transmitted by facsimile to the Patent and Trademark Office.

Depositor's Name: Sara R. Hart
(type or print name)

Signature: Sara R. Hart

Date: August 24, 2006

PTO/SB/21

Patent and Trademark Office
PATENT

RECEIVED
CENTRAL FAX CENTER

AUG 2 4 2006

APPEAL BRIEF TRANSMITTAL

Mail Stop Appeal-Brief Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Customer No.: 23696
Attorney Docket No.: 010055B1
In Re Application of: Roy Quick et al.
Serial Number: 09/863,139
Filed: May 22, 2001
Examiner: Moorthy, Aravind K.
Group Art Unit: 2131

Dear Sir:

Transmitted herewith for filing is a Notice of Appeal in the above identified application.

EXTENSION FEES	☐ One Month	$120	$
	☐ Two Months	$450	$
	☐ Three Months	$1020	$
	☒ Four Months	$ 1,590.00	$1,590.00
APPEAL BRIEF		$500	$500.00
TERMINAL DISCLAIMER		$130	$
		TOTAL FEE	$2,090.00

4. ☐ Fee check in the amount of $_____ is enclosed to pay for any claim and/or extension fees.
5. ☒ Please charge Deposit Account No. 17-0026 of QUALCOMM Incorporated the amount of $2,090.00
   The Commissioner is hereby authorized to charge payment of any additional fees that may be required, or credit any overpayment to said Deposit Account No. 17-0026. A duplicate of this sheet is enclosed for fee processing.
6. ☒ The Commissioner is further hereby authorized to charge to said Deposit Account No. 17-0026, pursuant to 37 CFR 1.25(b), any fee whatsoever which may become properly due or payable, as set forth in 37 CFR 1.16 to 37 CFR 1.18 inclusive, for the entire pendency of this application without specific additional authorization.

Date: August 24, 2006

Signature: David Hoffman Reg. No. 56771 for
Jae-Hee Choi, Reg. No. 45,288
(858) 651-5469

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-5787
Facsimile: (858) 658-2502

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8(a))

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

☐ deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Depositor's Name: _____
(type or print name)

Date: _____

FACSIMILE

☒ transmitted by facsimile to the Patent and Trademark Office.

Depositor's Name: Sara R. Hart
(type or print name)

Signature: Sara R. Hart

Date: August 24, 2006

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of	: Roy Quick et al.
Appl. No.	: 09/863,139
Filed	: May 22, 2001
Art Unit	: 2131
Examiner	: Moorthy, Aravind K.
Title	: Local Authentication in a Communication System
Attorney Docket No.	: 010055B1

MS Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' BRIEF

This is an appeal from the final Office Action dated August 24, 2005, rejecting claims 1-17.

(1) REAL PARTY IN INTEREST

The real party in interest is Qualcomm Incorporated, the assignee of the entire interest.

(2) RELATED APPEALS AND INTERFERENCES

Appellants are not aware of any related appeals, interferences or judicial proceedings.

(3) STATUS OF CLAIMS

The application was filed on May 22, 2001 with seventeen (17) claims, of which Claims 1, 8, 11, 15 and 17 are independent

All of the claims were rejected in the non-final Office Action dated November 24, 2003.

In Appellants' response dated February 24, 2004, arguments were made indicating the patentability of Claims 1-17 over the proffered references.

The Examiner rejected all the claims in the final Office Action dated May 12, 2004.

On February November 10, 2004, Appellants requested a continued examination and arguments were made indicating the patentability of Claims 1-17 over the proffered references.

Based on new grounds, all of the claims were rejected in the non-final Office Action dated February 7, 2005.

In Appellants' response dated June 7, 2005, arguments were made indicating the patentability of Claims 1-17 over the new references.

The Examiner rejected all the claims in the final Office Action dated August 24, 2005.

In Appellants' response dated January 23, 2006, arguments were made indicating the patentability of Claims 1-17 over the proffered references.

The Examiner, in the Advisory Action dated February 7, 2006, asserted that Appellants' arguments were not persuasive.

Appellants filed a Notice of Appeal dated February 24, 2005.

The status of the claims is as follows:

Claims rejected: Claims 1-17

Claims allowed: none

Claims withdrawn: none

Claims objected to: none

Claims canceled: none

Claims appealed: Claims 1-17

(4) STATUS OF AMENDMENTS

No amendment to the claims has been submitted since the final Office Action dated August 24, 2005.

(5) SUMMARY OF CLAIMED SUBJECT MATTER

Independent Claim 1 provides:

A subscriber identification module for providing local authentication of a subscriber in a communication system, comprising: a memory; and a processor configured to implement a set of instructions stored in the memory (Specification page 16, lines 15-30), the set of instructions for: generating a plurality of keys in response to

a received challenge (Specification page 12, lines 12-15); generating an initial value based upon a first key from the plurality of keys (Specification page 12, lines 25-28, page 13, lines 22-23, and Figure 5, element 511); concatenating the initial value with a received signal to form an input value (Specification page 13, lines 25-27 and Figure 5, element 512), wherein the received signal is transmitted from a communications unit communicatively coupled to the subscriber identification module, and the received signal is generated by the communications unit using a second key from the plurality of keys, the second key having been communicated from the subscriber identification module to the communications unit (Specification page 12, lines 18-25, page 13, lines 5-14, and Figure 5, elements 501-510); hashing the input value to form an authentication signal (Specification page 12, lines 25-29, page 13, lines 25-27, and Figure 5, element 513); and transmitting the authentication signal to the communications system via the communications unit (Specification page 12, lines 31-32, page 13, lines 28-30, and Figure 5, element 514).

Independent Claim 8 provides:

A subscriber identification module, comprising: a key generation element (Specification page 10, lines 1-4, page 12, lines 12-5 and element 250 of Figures 3 and 4); and a signature generator configured to receive a secret key from the key generation element and information from a mobile unit, and further configured to generate a signature that will be sent to the mobile unit, wherein the signature is generated by concatenating the secret key with the information from the mobile unit and hashing the concatenated secret key and information (Specification page 10, lines 11-14, page 12, lines 23-28, page 13, lines 21-27, and element 360 of Figures 3 and 4).

Independent Claim 11 provides:

An apparatus for providing secure local authentication of a subscriber in a communication system, comprising a subscriber identification module configured to interact with a communications unit, wherein the subscriber identification module comprises: a key generator for generating a plurality of keys from a received value and

a secret value (Specification page 10, lines 1-4, page 12, lines 12-5 and element 250 of Figures 3 and 4), wherein at least one communication key from the plurality of keys is delivered to the communications unit and at least one secret key from the plurality of keys is not delivered to the communications unit (Specification elements 310 and 320 of Figures 3 and 4); and a signature generator for generating an authorization signal from hashing a version of the at least one secret key together with an authorization message, wherein the authorization message is generated by the communications unit using a version of the at least one communication key (Specification page 10, lines 12-14, page 12, lines 23-28, page 13, lines 21-27, and element 360 of Figures 3 and 4).

Independent Claim 15 provides:

A method for providing authentication of a subscriber using a subscriber identification device, comprising: generating a plurality of keys (Specification page 10, lines 1-4, page 12, lines 12-15); transmitting at least one key from the plurality of keys to a communications device communicatively coupled to the subscriber identification device and holding private at least one key from the plurality of keys (Specification elements 310 and 320 of Figures 3 and 4); generating a signature at the communications device using both the at least one key transmitted to the communications device and a transmission message, wherein generating is implemented by hashing a concatenated value formed from the at least one key and the transmission message (Specification page 10, lines 7-11, page 12, lines 18-21, page 13, lines 5-14, Figure 5, elements 504-505); transmitting the signature to the subscriber identification device (Specification page 10, lines 11-12, page 12, lines 23-25, page 13, lines 21-22 and Figure 5, element 510); receiving the signature at the subscriber identification device; generating a primary signature from the received signature, wherein the generating is implemented by hashing a concatenated value formed from the at least one private key and the signature received from the communications device (Specification page 10, lines 12-13, page 12, lines 25-29, page 13, lines 22-28, and Figure 5, elements 512 and 513); and conveying the primary signature to a communications system (Specification page 10, lines 14-16, page 12, lines 31-32, page

13, lines 28-30, and Figure 5, element 514).

Independent Claim 17 provides:

An apparatus for authenticating a subscriber in a wireless communication system, wherein the apparatus can be communicatively coupled to a mobile station operating within the wireless communications system, comprising: a memory; and a processor configured to implement a set of instructions stored in the memory (Specification page 16, lines 15-30), the set of instructions for selectively generating a primary signature based upon a key that is held private from the mobile station and a secondary signature that is received from the mobile station (Specification page 10, lines 11-16 and Figure 3, elements 320 and 340).

(6) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 2 and 5 under 35 U.S.C. §102(e) as being allegedly anticipated by U.S. Patent No. 6,609,199 issued to DeTreville (hereinafter "DeTreville")

Claims 8-13, 15 and 17 under 35 U.S.C. §102(e) as being allegedly anticipated by U.S. Patent No. 6,516,414 issued to Zhang et al. (hereinafter "Zhang").

Claims 3, 4, 6 and 7 under 35 U.S.C. §103 as being unpatentable over DeTreville in view of U.S. Patent No. 6,076,162 issued to Deindl et al. (hereinafter "Deindl").

Claims 14 and 16 under 35 U.S.C. §103 as being unpatentable over Zhang in view of Applied Cryptography (hereinafter Schneier).

(7) ARGUMENT

I. 35 U.S.C. § 102(e) Rejections

To anticipate a claim under 35 U.S.C. §102(e), the reference must teach every element of the claim and "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." (see MPEP §2131).

A. Claims 1, 2 and 5

The issue is whether the Examiner has properly rejected Claims 1, 2 and 5 under 35 U.S.C. § 102(e) as being allegedly anticipated by U.S. Patent No. 6,609,199 issued to DeTreville.

In the final Office Action dated August 24, 2005, the Examiner states that DeTreville teaches generating a plurality of keys in response to a received challenge from the portable IC device and, more particularly, cites column 5, lines 54-65. Appellants respectfully disagree with the characterization of DeTreville for the following reasons.

DeTreville discusses an authenticated boot methodology in which an operating system of a computer proves its identity to a microprocessor to certify that it is trusted. DeTreville teaches using the authenticated boot for the mutual authentication between an IC device 116 and a public computer that is accessible by the public (col. 4, lines 35 to 54). Particularly, the portion cited by the Examiner discloses the "*CPU manufacturer equips the CPU 134 with a pair of public and private keys 150 that is unique to the CPU.*" "*The private key is never revealed and is used only for the specific purposes of signing stylized states, such as when responding to challenges from a portable IC device.*" (See col. 5, lines 54 to 65).

In other words, DeTreville teaches CPU manufacturer to equip the CPU with a pair of public and private key. Accordingly, the keys are stored onto the CPU at the time of manufacturing. The already stored private key is then use when responding to challenges from a portable IC device. This means that the keys, i.e. the public and/or private keys, are not generated in response to a received challenge. The keys are used in response to a received challenge. Therefore, DeTreville does not teach or even suggest generating a plurality of keys in response to a received challenge.

In the Advisory Action dated February 7, 2006, the Examiner asserts that the generation of the public/private key is generated in response to a challenge. For at least the foregoing reasons, Appellant submits that the public/private keys are not generated in response to a received challenge.

Also, the Examiner states that DeTreville discloses generating an initial value based upon a first key from the plurality of keys generated in response to a received challenge. Assuming for the purposes of argument that a plurality of keys are generated in response to a received challenge, DeTreville does not teach or even mention a generating an initial value based upon a first key from the plurality of keys. Particularly, the portion cited by the Examiner

states the "*SIR or the seed field 222 holds an authenticate boot key generator seed. The CPU uses the seed in field 222 to generate keys unique to the OS and processor.*" (See col. 9, lines 14-16). Here, the SIR is defined as an internal software identity register which is cleared at the beginning of each boot. (See col. 6, lines 40-41). In other words, the SIR is neither the public key nor the private key that the Examiner asserts is generated in response to a received challenge. Moreover, the seed is not generated based upon the SIR. Rather, the SIR holds the seed to generated keys unique to the OS and the processor.

Additionally, for the purposes of further argument, assume that an initial value is generated based upon a first key from the plurality of keys. DeTrevillet teaches the use of a SIR by the CPU in executing an authenticated boot. The values of the SIR are set depending on whether a successful authenticated boot occurs (see col. 6, lines 40-51 and col. 8, lines 31-42). The CPU can then generate a signed certificate containing the resultant boot log data to attest to a particular operating system (see col. 9, lines 5-13). Fig. 6 shows a structure of the boot log data including the SIR or a seed field. DeTreville then teaches that the CPU can use the seed to generate keys unique to the OS and processor (see col. 9, lines 14-21). If this seed is considered an initial value generated based upon a key from a plurality of key, DeTreville still does not teach or even mention concatenating the initial value with a received signal that is generated using a second key from the plurality of keys generated in response to the challenge.

Since DeTreville does not teach at least the above elements of claim 1, Appellants submit that DeTreville does not teach all elements of claim 1 and therefore, claim 1 is allowable. Also, claims 2 and 5 depend from and include all the elements cited in the independent claim 1. Accordingly, Appellant submits that these claims are believed to be allowable based on their dependency from an allowable base claim as well as other novel features included therein.

For at least the foregoing reasons, Appellants respectfully request a withdrawal of the rejection under 35 U.S.C. §102.

B. Claims 8-10

The issue is whether the Examiner has properly rejected Claims 8-10 under 35 U.S.C. §102(e) as being allegedly anticipated by Zhang.

Zhang discusses an improved authorization process for a conditional access system (see Background). It teaches a trusted third party that generates and passes a list of public or secret keys of receiver devices to a service provider over a secure channel. The service provider uses

the list in the authentication of the respective receiver devices. Once authenticated, a receiver device may generate session keys to protect communications to the service provider (see col. 4, lines 35-64). The receiver device includes a host device and a point-of deployment module (see, col. 3, lines 12-15).

In the Advisory Action dated February 7, 2006, the Examiner asserts, without more, that Zhang discloses signature generation by hashing the concatenation of a secret key and the device identifier. However, the portion cited by the Examiner in the final Office Action dated August 24, 2005 discloses a host device, including a device identifier "H_ID", generating a random number M_H. The random number is concatenated with H_ID and concatenated value is transmitted to the POD module. The POD module, including a device identifier "P_ID", generates its random number M_P and transmits to the service provider a stream containing a concatenation of P_ID and H_ID. Based upon the stream, the service provider retrieves verification information and transmits a binding message to the POD module. The POD module processes the binding message. The processed binding message is concatenated with M_P and forwarded to the host device. (See col. 8, lines 32-67).

Accordingly, Zhang discloses concatenation performed with respect to a random number M_H or M_P, a device identifier P_ID or H_ID and a binding message $G^{-(P+H)} \bmod N$ (see col. 8, lines 32-62). Upon further review, Zhang discusses various cryptographic concepts (see col. 2, lines 17-40) and teaches a content protection system using concatenation of various parameters (see col. 7, line 7 to col. 8, line 1 and col. 8, lines 33-37).

There is nothing in Zhang to suggest a concatenation of a secret key with information from a mobile unit as in claim 8. While Zhang teaches concatenation of two values, there is nothing to suggest a concatenation of a secret key with information from a mobile unit. Thus, Zhang does not teach or even mention a signature generator configured to generate a signature by concatenating a secret key with information from a mobile unit as in claim 8.

Since Zhang does not teach at least the above elements of the respective claims, Appellant submit that Zhang does not teach all elements of the claims and therefore, claim 8 is allowable. Also, claims 9-10 depend from and include all the elements cited in the independent claims 8 and are believed to be allowable based on their dependency from an allowable base claim as well as other novel features included therein. For at least the foregoing reasons,

Appellant respectfully submit that Zhang does not teach every element of the claims and request a withdrawal of the rejection under 35 U.S.C. §102.

C. Claims 11-13

The issue is whether the Examiner has properly rejected Claims 11-13 under 35 U.S.C. §102(e) as being allegedly anticipated by Zhang.

In view of the discussion above, assuming for the purposes of argument that Zhang teaches generation of a plurality of keys, Zhang does not teach or even suggest a key generator for generating a plurality of keys from a received value and a secret value as in claim 11.

Zhang teaches derivation of shared key k and a shared session key K using the shared key k such that content for transmission can be ciphered using the shared session key K (see col. 12, lines 17-20, lines 34-39 and lines 45-54). Namely, both keys k and K are derived. This means that a communication key is not delivered. Therefore, Zhang does not teach delivering a communication key to a communications unit as in claim 11. In the portion cited by the Examiner, Zhang teaches computing a hash function with respect to a common initial counter value N and a secret key P or H (see col. 11, lines 50-53 and lines 55-56).

However, it does not teach or even mention a signature generator for generating an authorization signal from hashing a version of at least one secret key together with an authorization message.

Since Zhang does not teach at least the above elements of the respective claims, Appellant submit that Zhang does not teach all elements of the claims and therefore, claim 11 is allowable. Also, claims 12-13 depend from and include all the elements cited in the independent claim 11 and are believed to be allowable based on their dependency from an allowable base claim as well as other novel features included therein. For at least the foregoing reasons, Appellant respectfully submit that Zhang does not teach every element of the claims and request a withdrawal of the rejection under 35 U.S.C. §102.

D. Claim 15

The issue is whether the Examiner has properly rejected Claim 15 under 35 U.S.C. §102(e) as being allegedly anticipated by Zhang.

With respect to claim 15, Zhang teaches an authentication process in which the host device sends its ID and digital signature to the POD, and the POD sends its ID and digital signature as well as the information received from the host device to the head-end system. The head-end system compares the received information to verify that the host and POD are valid devices (see col. 13, lines 35-52). While Zhang mentions generation of signatures, it does not teach or suggest generating a signature by hashing a concatenated value formed from a key and a transmission message. Furthermore, Zhang does not teach or even mention generating a primary signature.

Since Zhang does not teach at least the above elements of the claim, Appellant submit that claim 15 is allowable. For at least the foregoing reasons, Appellant respectfully submit that Zhang does not teach every element of the claims and request a withdrawal of the rejection under 35 U.S.C. §102.

E. Claims 17

The issue is whether the Examiner has properly rejected Claims 8-13, 15 and 17 under 35 U.S.C. §102(e) as being allegedly anticipated by Zhang.

Based upon the discussion above, Zhang does not teach or even suggest an apparatus coupled to a mobile station, wherein the apparatus comprises a processor configured to generate a primary signature based on a key that is held private from the mobile station and a secondary signature that is received from the mobile station as in claim 17. The portion cited by the Examiner discusses generation of session keys. It does not discuss an apparatus communicatively coupled to a mobile station, wherein the apparatus comprises a memory and a processor.

In the Advisory Action dated February 7, 2006, the Examiner states that the POD module creates the primary signature with its own private key and the secondary signature is created with the private key of the host device. However, it is unclear what the Examiner is considering as the primary signature and secondary signature. In relation to the primary and secondary signatures, it is also unclear what the Examiner is considering as the mobile station. It should be noted that the host device is an integrated receiver device such as a set-top box and the POD is a condition access module (see col. 3, lines 12-15). As a result, assuming for the purposes of argument that the POD is a mobile station, there is no suggestion that the host device generates

the primary signature based upon a key that is held private from the POD and a secondary signature that is received from the POD.

Since Zhang does not teach at least the above elements of the claim, Appellant submit that claim 17 is allowable. For at least the foregoing reasons, Appellants respectfully request a withdrawal of the rejection under 35 U.S.C. §102.

II. 35 U.S.C. § 103 Rejections

To establish a prima facie case of obviousness for a claimed invention, all the claim elements must be taught or suggested by the prior art. (MPEP 2143.03)

A. Claims 3, 4, 6 and 7

The issue is whether the Examiner has properly rejected Claims 3, 4, 6 and 7 under 35 U.S.C. §103 as being unpatentable over DeTreville in view of Deindl.

Claims 3, 4, 6 and 7 depend from and include all the elements cited in the independent claim 1. Accordingly, Appellent submits that DeTreville does not disclose every element of claims 3, 4, 6 and 7 based on its dependency from claim 1 as well as other novel features included therein. Upon review, Deindl also does not teach the generation of a plurality of keys, the generation of an initial value and the concatenation as in independent claim 1.

Since neither DeTreville nor Deindl, separately or combined, teach or suggest all the elements, Appellants respectfully submit that the Examiner has failed to set forth a prima facie case of obviousness and respectfully requests that the rejections of claims 3, 4, 6 and 7 be withdrawn.

B. Claim 14

The issue is whether the Examiner has properly rejected Claim 14 under 35 U.S.C. §103 as being unpatentable over DeTreville in view of Schneier.

Claim 14 depend from and include all the elements cited in the independent claims 11. Accordingly, Appellent submits that Zhang does not disclose every element of claim 14 based on its dependency from claim 11 as well as other novel features included therein. Upon review,

Schneier also does not teach the generation of a plurality of keys, the generation of a signature as in independent claim 11.

Therefore, since neither Zhang nor Schneier, separately or combined, teach or suggest all the elements, Appellant respectfully submit that the Examiner has failed to set forth a prima facie case of obviousness and respectfully requests that the rejections of claim 14 be withdrawn.

C. Claim 16

The issue is whether the Examiner has properly rejected Claim 16 under 35 U.S.C. §103 as being unpatentable over DeTreville in view of Schneier.

Claim 16 depend from and include all the elements cited in the independent claims 15. Accordingly, Appellent submits that Zhang does not disclose every element of claim 16 based on its dependency from claim 15 as well as other novel features included therein. Upon review, Schneier also does not teach the generation of a signature as in independent claim 15.

Therefore, since neither Zhang nor Schneier, separately or combined, teach or suggest all the elements, Appellant respectfully submit that the Examiner has failed to set forth a prima facie case of obviousness and respectfully requests that the rejections of claims 14 and 16 be withdrawn.

III. Conclusion

For the foregoing reasons, it is respectfully submitted that in each of the rejections discussed herein under 35 U.S.C. § 102(e) and 103, the Examiner has failed to show that the proffered references teach or suggest each and every element of the claimed invention. Accordingly, reversal of all outstanding rejections is earnestly solicited.

Respectfully submitted,
QUALCOMM Incorporated,

Dated: August 24, 2006

By: David Hilfiker Reg. No. 56,771 for
Jae-Hee Choi, Reg. No. 45,288
Phone: (858) 651-5469

(8) CLAIMS APPENDIX

1. (Original) A subscriber identification module for providing local authentication of a subscriber in a communication system, comprising:

a memory; and

a processor configured to implement a set of instructions stored in the memory, the set of instructions for:

generating a plurality of keys in response to a received challenge;

generating an initial value based upon a first key from the plurality of keys;

concatenating the initial value with a received signal to form an input value, wherein the received signal is transmitted from a communications unit communicatively coupled to the subscriber identification module, and the received signal is generated by the communications unit using a second key from the plurality of keys, the second key having been communicated from the subscriber identification module to the communications unit;

hashing the input value to form an authentication signal; and

transmitting the authentication signal to the communications system via the communications unit.

2. (Original) The apparatus of Claim 1, wherein hashing the input value is performed in accordance with the Secure Hashing Algorithm (SHA-1).

3. (Original) The apparatus of Claim 1, wherein generating the initial value comprises padding the first key.

4. (Original) The apparatus of Claim 3, wherein generating the initial value further comprises adding the padded first key bit-wise to a constant value.

5. (Original) The apparatus of Claim 1, wherein the received signal is generated at the communications unit by:

receiving the second key from the subscriber identification module;

generating a local initial value based upon the second key;

concatenating the local initial value and a message to form a local input value;

hashing the local input value to form the received signal; and

transmitting the received signal to the subscriber identification module.

6. (Original) The apparatus of Claim 5, wherein generating the local initial value comprises padding the second key.

7. (Original) The apparatus of Claim 6, wherein generating the local initial value further comprises adding the padded second key bit-wise to a second constant value.

8. (Original) A subscriber identification module, comprising:

a key generation element; and

a signature generator configured to receive a secret key from the key generation element and information from a mobile unit, and further configured to generate a signature that will be sent to the mobile unit, wherein the signature is generated by concatenating the secret key with the information from the mobile unit and hashing the concatenated secret key and information.

9. (Original) The subscriber identification module of Claim 8, wherein the key generation element comprises:

a memory; and

a processor configured to execute a set of instructions stored in the memory, wherein the set of instructions performs a cryptographic transformation upon an input value to produce a plurality of temporary keys.

10. (Original) The subscriber identification module of Claim 9, wherein the cryptographic transformation is performed using a permanent key.

11. (Original) An apparatus for providing secure local authentication of a subscriber in a communication system, comprising a subscriber identification module configured to interact with a communications unit, wherein the subscriber identification module comprises:

a key generator for generating a plurality of keys from a received value and a secret value, wherein at least one communication key from the plurality of keys is delivered to the communications unit and at least one secret key from the plurality of keys is not delivered to the communications unit; and

a signature generator for generating an authorization signal from hashing a version of the at least one secret key together with an authorization message, wherein the authorization message is generated by the communications unit using a version of the at least one communication key.

12. (Original) The apparatus of Claim 11, wherein the subscriber identification module is configured to be inserted into the communications unit.

13. (Original) The apparatus of Claim 11, wherein the at least one communication key comprises an integrity key.

14. (Original) The apparatus of Claim 11, wherein hashing is performed in accordance with SHA-1.

15. (Original) A method for providing authentication of a subscriber using a subscriber identification device, comprising:

generating a plurality of keys;

transmitting at least one key from the plurality of keys to a communications device communicatively coupled to the subscriber identification device and holding private at least one key from the plurality of keys;

generating a signature at the communications device using both the at least one key transmitted to the communications device and a transmission message, wherein generating is implemented by hashing a concatenated value formed from the at least one key and the transmission message;

transmitting the signature to the subscriber identification device;

receiving the signature at the subscriber identification device;

generating a primary signature from the received signature, wherein the generating is implemented by hashing a concatenated value formed from the at least one private key and the signature received from the communications device; and

conveying the primary signature to a communications system.

16. (Original) The method of Claim 15, wherein hashing is implemented in accordance with SHA-1.

17. (Original) An apparatus for authenticating a subscriber in a wireless communication system, wherein the apparatus can be communicatively coupled to a mobile station operating within the wireless communications system, comprising:

a memory; and

a processor configured to implement a set of instructions stored in the memory, the set of instructions for selectively generating a primary signature based upon a key that is held private from the mobile station and a secondary signature that is received from the mobile station.

(9) EVIDENCE APPENDIX

None

(10) RELATED PROCEEDINGS APPENDIX

None